

# ATTACHMENT 2

AO 106 (Rev. 04/10) Application for a Search Warrant

## UNITED STATES DISTRICT COURT

for the  
District of MassachusettsIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)The Residence at 64 Plymouth Drive, Apartment C,  
Norwood, Massachusetts, as More Fully Described in  
Attachment A, Which is Incorporated by Reference

Case No. 15-MJ-2187-MBB

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Residence at 64 Plymouth Drive, Apartment C, Norwood, Massachusetts, as More Fully Described in Attachment A, Which is Incorporated by Reference

located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated by reference, for a list property to be seized.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section                         | Offense Description             |
|--------------------------------------|---------------------------------|
| 8 U.S.C. § 2252A(a)(2)(A) and (b)(1) | receipt of child pornography    |
| 18 U.S.C. § 2252A(a)(5)(B) and       | possession of child pornography |

The application is based on these facts:

See the attached Affidavit of Federal Bureau of Investigation Task Force Officer Michael Sullivan, which is incorporated by reference.

☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 08/11/2015City and state: Boston, Massachusetts
  
 MICHAEL SULLIVAN, Task Force Officer  

  
 HON. MARIANNE B. BOWLER, U.S. Magistrate Judge  
 Printed name and title

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

**INTRODUCTION**

I, Michael Sullivan, having been first duly sworn, do hereby depose and state as follows:

1. I am employed as a Detective with the City of Boston (Massachusetts) Police Department. I am also a sworn Special Deputy United States Marshal. I have been employed by the Boston Police Department approximately the past nine years and am currently assigned as a Task Force Officer to the FBI Boston Division, Child Exploitation Task Force. While employed by the Boston Police Department, I have investigated state and federal criminal violations related to, among other things, the on-line sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.
2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of or access with intent to view child pornography), are located within 64 Plymouth Drive, Apartment C, in Norwood Massachusetts (hereinafter the "SUBJECT PREMISES"). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachment A, incorporated herein by reference. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Detective with the Boston Police Department. Because this affidavit is submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

#### **BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE**

4. A user of the Internet account at the Subject Premises has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as "Website A."<sup>1</sup> There is probable cause to believe that a user of the Internet account at the Subject Premises knowingly received and distributed child pornography on "Website A."

---

<sup>1</sup> The actual name of "Website A" is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "Website A."

### The Network<sup>2</sup>

5. “Website A” operated on a network (“the Network”) available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user’s existing web browser, downloading free software available from the Network’s administrators, or downloading a publicly-available third-party application.<sup>3</sup> Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user’s physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

6. Websites that are accessible only to users within the Network can be set up within the Network and “Website A” was one such website. Accordingly, “Website A” could not generally be accessed through the traditional Internet.<sup>4</sup> Only a user who had installed the appropriate software on the user’s computer could access “Website A.” Even after connecting to the Network, however, a user had to know the exact web address of “Website A” in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike

---

<sup>2</sup> The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as “the Network.”

<sup>3</sup> Users may also access the Network through so-called “gateways” on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

<sup>4</sup> Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact

on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

7. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user.

8. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

Description of "Website A" and its Content

9. "Website A" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting "Website A" was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

10. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two

---

about February 20, 2015, Website A was no longer accessible through the traditional Internet.

data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

11. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

12. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

13. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and

experience, I know that "jailbait" refers to underage but post-pubescent minors; the abbreviation "HC" means hardcore (i.e., depictions of penetrative sexually explicit conduct); and "scat" refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

14. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The "last post" section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

15. A review of the various topics within the "[Website A] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

16. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

- (a) On February 3, 2015, a user posted a topic entitled "Buratino-06" in the forum "Pre-

teen – Videos - Girls HC” that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

(b) On January 30, 2015, a user posted a topic entitled “Sammy” in the forum “Pre-teen – Photos – Girls” that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and

(c) On September 16, 2014, a user posted a topic entitled “9yo Niece - Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

17. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, “Website A” contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

18. “Website A” also included a feature referred to as “[Website A] Image Hosting.” This feature of “Website A” allowed users of “Website A” to upload links to images of child pornography

that are accessible to all registered users of "Website A." On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita" which was created by a particular "Website A" user. The post contained links to images stored on "[Website A] Image Hosting." The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

19. Text sections of "Website A" provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse.

- a. On January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

#### Court Authorized Use of Network Investigative Technique

20. Websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A publicly available lookup could then be

performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

21. However, because of the Network software utilized by "Website A," any such logs of user activity would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of "Website A."

22. Accordingly, on February 20, 2015, the same date "Website A" was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A." Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of

other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

"Manakarlupa" on "Website A"

23. According to data obtained from logs on "Website A," monitoring by law enforcement and the deployment of a NIT, a user with the user name "Manakarlupa" engaged in the following activity on "Website A."

24. The profile page of user "Manakarlupa" indicated this user originally registered an account on "Website A" on February 10, 2015. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user "Manakarlupa's" profile, this user was a normal member of "Website A." Further, according to the statistics section of this user's profile, the user "Manakarlupa" had been actively logged into the website for a total of 2 hours, 19 minutes and 35 seconds between the dates of February 10, 2015 and March 4, 2015. In addition the user added the personal text of "watch out Playpen newbie here".

25. On March 4, 2015, the user "Manakarlupa" with IP address 108.20.181.106 accessed a forum entitled, "Strawberry Shortcake Reuped on 03/04/2015". Among other things, this post contained a link to an image (.jpg file) of a picture collage that depicted a pre-pubescent female, about five to seven years old, posed in a variety of poses that the focal point of the picture was the child's vagina, anus, and one that had a penis placed against her mouth.

26. On March 4, 2015, "Manakarlupa" accessed a file entitled "Estefy (Latina Anal) Deep anal creampie - asi se mama linda.3gp". The file contained 1 image that contained a collage of images of a prepubescent female performing oral sex and anal sex with an adult male.

IP Address and Identification of User "Manakarlupa" on "Website A"

27. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on February 23, 2015, the user "Manakarlupa" accessed "Website A" from IP address 108.20.181.106.

28. Using publicly available websites, FBI Special Agents were able to determine that the above IP Address was operated by the Internet Service Provider ("ISP") Verizon. Deployment of the NIT also allowed the FBI to gather identifying information on the user's computer. The information for "Manakarlupa" computer included host and log on names, "Alex-PC" and "Alex."

29. In March 2015, the FBI served an administrative subpoena to Verizon requesting information related to the user who was assigned IP address 108.20.181.106 as of February 23, 2015. According to the information received from Verizon, the subscriber, Alex Levin, is receiving Internet service at the address of the SUBJECT PREMISES with an account creation date of November 14, 2011.

30. The FBI conducted a database search of public records for the SUBJECT PREMISES, 64 Plymouth Drive, Apartment C, in Norwood, Massachusetts. The search listed Alex Levin, DOB 07/01/1961 as a resident of 64 Plymouth Drive, Apartment C, in Norwood, Massachusetts. A check of the MA Registry of Motor Vehicles ("RMV") showed Alex Levin listed at 64 Plymouth Drive, Apartment C, Norwood, Massachusetts as a mailing address and did not report any home address.

31. On or about August 10, 2015 representatives of the United States Postal Inspection Service (USPIS) reported that Alex Levin is only person known to them currently receiving mail

at 64 Plymouth Drive, Apartment C (Suite C), Norwood, Massachusetts.

32. On July 14, 2015, I observed a mailbox in the front lobby of 64 Plymouth Drive that was labeled "LEVIN" and "C".

33. On July 14, 2015, I observed a black Jeep Wrangler, MA registration 9270CF, parked in the parking lot behind SUBJECT PREMISES. A check with the MA RMV showed the vehicle as registered to Alex Levin.

34. On August 5, 2015, I conducted a search of the available wireless networks in the area of the SUBJECT PREMISES which showed the following:

| <u>Network</u>         | <u>Status</u> |
|------------------------|---------------|
| 97RH5                  | Locked        |
| belin.0da              | Locked        |
| Cisco68290             | Locked        |
| HOME-57C6-2.4          | Locked        |
| HOME-57C6-5            | Locked        |
| HP-Print-16-Officej... | Locked        |
| WIN-6KQ3080VBN...      | Locked        |
| xfinitywifi            | Unlocked      |
| XKMHJ                  | Locked        |
| YY5F9                  | Locked        |
| ZUCG5                  | Locked        |

Based upon my training and experience, I know that xfinitywifi, the only wireless network in the area of the SUBJECT PREMISES, as of August 5, 2015, that showed an unlocked status, is an xfinity hotspot that is available to users of Comcast and not Verizon, the ISP that operates the subject IP address.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT  
TO VIEW AND POSSESS, COLLECT, RECEIVE, OR DISTRIBUTE CHILD  
PORNOGRAPHY**

35. Based on my previous investigative experience related to child pornography investigations,

and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view and possess, collect, receive or distribute images of child pornography:

- a. Individuals who access with intent to view and possess, collect, receive or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals who access with intent to view and possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who access with intent to view and possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and

videotapes for many years.

d. Likewise, individuals who access with intent to view and possess, collect, receive or distribute child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who access with intent to view and possess, collect, receive or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, Internet Relay Chat or chat rooms, have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who access with intent to view and possess, collect, receive or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the

investigation of child pornography throughout the world.

34. Based upon the foregoing, I believe that a user of the Internet account at SUBJECT PREMISES likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography.

#### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

35. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

36. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

37. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically

changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

38. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

39. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

40. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online

storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

41. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

42. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to

examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

43. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

44. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

**SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA**

45. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;
- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.


#### CONCLUSION

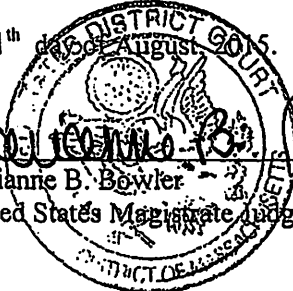
46. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this

Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.


  
Task Force Officer Michael Sullivan  
Federal Bureau of Investigation


Sworn and subscribed to before me this 11<sup>th</sup> day of August, 2015.

  
Marianne B. Bowler  
United States Magistrate Judge



I have reviewed the images referenced in paragraphs 25 and 26 above, and I find probable cause to believe that the images constitute child pornography. The Affiant shall continue to preserve the image files and screen capture images provided to the Court, for the duration of the pendency of this matter, including any relevant appeal process.

  
HON. MARIANNE B. BOWLER  
United States Magistrate Judge



ATTACHMENT A

**DESCRIPTION OF THE LOCATION TO BE SEARCHED**

The SUBJECT PREMISES is located at 64 Plymouth Drive, Apartment C, Norwood, Massachusetts. The location 64 Plymouth Drive is a three story brick apartment building with white trim with a white front door and the number "64" clearly displayed above the door. The rear door of 64 Plymouth Drive is also clearly marked with the number "64." Apartment C is located on the ground level and most easily accessed by entering through the rear door down a series of stairs. At the bottom of these stairs, Apartment C is the first door on the left. The front door to Apartment C is blue and engraved on the door knocker is the letter "C."



**ATTACHMENT B**

**Information to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - h. evidence of the times the COMPUTER was used;
  - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - k. records of or information about Internet Protocol addresses used by the COMPUTER;
  - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
  - m. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including
- a. Records, information, and items relating to the occupancy or ownership of 64 Plymouth Drive, Apartment C, Norwood, Massachusetts including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes; and
  - b. Records and information relating to sexual exploitation of children, including correspondence and communications between users of "Website A."

As used above, the terms "records" and "information" includes all forms of creation or

storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.